AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Currently Amended): A system for detection and blocking of IP collisions, comprising:

~~a communication interface and communication kernel module that provides a communication interface that enables a collided IP detection system to share information with other hosts and provides a kernel for controlling the communication;~~

~~a network interface driver module that is connected with a physical device that is a network interface and an upper communication module to transmit packets to the network, and transmits packets collected in the network to the upper communication module;~~

~~a network interface module that is connected to the devices connected to the network;~~

a packet capture driver module that collects all packets detected in ~~the~~ a network;

an ARP packet filtering module that filters only ARP packets among the packets being captured from the packet capture driver module;

an IP collision decision module that determines if ~~the collected packets are~~ a filtered ARP packet is collided IP packets or not and, if ~~so~~ it is, transmits the results to a listing module;

an access blocking decision module that notifies an access status ~~if an~~ when the filtered ARP packet is an ARP request packet and the ARP request packet is included in an access blocking policy list;

an access blocking module that, depending on the access blocking decision module's decision to block the access on a particular packet, blocks ~~the~~ network access by transmitting an ARP respond packet ~~to the blocked~~ in response to the particular packet;

a data storage module that stores information set to operate the collided IP detection system, a detected collided IP list, and a newly detected host's IP and MAC address lists;

a search list logging and saving module that internally lists ~~the~~ detected collided IP data and periodically ~~it~~ saves it in a storage medium; and a detection result notification module that transmits the detected collided IP data to another system and notifies ~~the~~ an administrator of it,

~~wherein when the ARP packet is collected from the network, each ARP packet is classified into a request packet and a respond packet after being identified, and then if it is a new request packet, it is added to the list, but if it is a respond packet that also exists in input request ARP packet list, the packet's collision is detected and at the same time the ARP packet's access is blocked~~

wherein the IP collision decision module determines if the number of ARP respond packets occurring by each IP exceeds a reference number set within a predefined time out period, and confirms the ARP packet as IP collision and adds the ARP packet to a list if the number of ARP respond packets occurring by each IP exceeds the set reference number, and the IP collision decision module determines IP collisions for all IPs.

Claim 2 (Currently Amended): A method of detecting IP collisions using an IP collision detection system between a client and a server, comprising the steps of:

(a) collecting all packets created by accessing ~~the~~ a network;

(b) filtering only ARP packets among the collected packets;

(c) determining whether ~~the~~ a filtered ARP packet is an ARP request packet or an ARP respond packet;

(d) adding a MAC address to a list by IP address if the filtered ARP packet is an ARP request packet;

(e) incrementing a count by one each time if the filtered ARP packet is an ARP respond packet;

(f) determining if the number of ~~the~~ ARP respond packets occurring by each IP exceeds ~~the frequency~~ a reference number set within a predefined time out period, and if ~~it~~ the number of ARP respond packets occurring by each IP exceeds the set ~~frequency~~ reference number, confirming ~~it~~ the ARP packet as IP collision and adding ~~it~~ the ARP packet to ~~the~~ a list; and

(g) resetting each IP's counter if the number of the ARP respond packets occurring are less than the set ~~frequency, resetting each IP's counter~~ reference,

wherein step (f) is executed on all IPs to detect IP collisions for all IPs.

Claim 3 (Currently Amended): ~~A~~ The method of ~~blocking collided IP using an IP collision blocking system between a client and a server,~~ claim 2, further comprising the steps of:

~~collecting all packets transmitted over a network;~~

~~filtering only ARP packets among the collected packets;~~

~~determining whether the filtered ARP packet is an ARP request packet or an ARP respond packet;~~

confirming if an IP address ~~and~~ or IP or MAC are included in a block policy list if the filtered ARP packet is an ARP request packet;

unicasting ~~the~~ an ARP respond packet to block access to a corresponding host if an ARP request packet is included in the block policy list; and

broadcasting the ARP respond packet to block access after unicasting the ARP respond packet, wherein ~~thereby blocking~~ the network access is thereby blocked.